General Services Administration (GSA) Infrastructure and Communications Solutions (GICS)

Task Order #47QTCB20F0006

Fair Opportunity using the General Services Administration's Enterprise Infrastructure Solutions (EIS) Contract

6/19/2020

SECTION C: DESCRIPTION/SPECIFICATIONS/STATEMENT OF WORK

This is the General Services Administration (GSA) solicitation for services utilizing GSA's Enterprise Infrastructure Solutions (EIS) contract.

This solicitation describes the full range of agency-specific requirements. The requirements for the services sought herein are defined in **Section C** of the EIS contract. GSA expects that all EIS contractors provide the baseline level of service and support specified in the EIS contract.

The contractor shall provide all personnel, transportation, equipment, tools, materials, supplies, installation, management, supervision, engineering, maintenance, testing, and services necessary to make circuits/services fully operational and to perform all tasks and functions as defined in this solicitation.

The contractor shall deliver and support the service(s) described in this section as well as required SRE and appropriate labor categories necessary to implement and manage the service.

C.1 Background

GSA currently provides data, voice, video services, and essential enterprise applications to approximately 14,000 end-users (i.e., employees and contractors) who leverage its network infrastructure to conduct official business. GSA's full employee population is approximately 17,000, but not all employees use all services, making 14,000 a better estimate. GSA also provides information technology support services to a small number of external agencies, committees, and government entities. GSA users are located in more than 800 CONUS and OCONUS locations, including Alaska, Guam, Hawaii, Puerto Rico, Saipan, U.S. Virgin Islands, and non-domestic (international) sites on U.S. military facilities/bases, including approximately 20 locations in Europe (e.g., Germany, Italy, Belgium), and several locations in Asia (e.g., Japan, Korea). Many GSA end-users regularly telework, travel or work from remote locations.

The network infrastructure that supports GSA's mission and programs is composed of a Multiprotocol Label Switching (MPLS) wide area network (WAN), high-speed gigabit local area network (LAN), multi-tiered security fabric, and remote access technologies. The MPLS WAN is based on a legacy hub and spoke architecture that connects GSA core sites of Regional Office Buildings (ROBs), Central Office (CO), large Field Offices (FOs) and two data centers. The network is critical for the day-to-day operations of all GSA lines-of-business (LOBs) and is available 24x7x365.

The purpose of this solicitation is to transition the like-for-like services procured from the GSA Networx, Washington Interagency Telecommunications System 3 (WITS 3), and Regional Services Local Service Agreements (LSAs) to the GSA EIS contract by May 31, 2021 for task orders 1 and 2. Transformation services proposed for task orders 1 and 2 must have a service initiation date no later than March 31, 2022. For task order 3, completion of all transition activities must be completed by July 30, 2022.

GSA is in a declining budget environment and is looking to EIS contractors to assist with reducing capital and operating expenditures associated with transitioning to the EIS contract, and in future service deliveries. Further, GSA is looking for EIS contractors to propose solutions and deliver services that enable GSA to maintain a relatively flat or declining spend for task order years 1 through 5.

C.1.1 Services Sought

GSA seeks to acquire the following EIS service(s):

- Data Services
- Voice Services
- Colocated Hosting Services
- Managed Services
- Access Arrangements
- Service Related Labor
- Service Related Equipment
- Cable and Wiring
- National Security and Emergency Preparedness

C.1.2 Project Overview

GSA is seeking to transition to EIS in phases to transform its network without any service interruption. The transition to EIS will allow GSA to get consistent support services with high availability and resilience to meet its mission.

Throughout the task order(s) period of performance, after the initial transition phase, GSA plans to gradually transform its network to take advantage of advances in technology to achieve better services at lower prices, and reduce operational risk and cost. During the initial transition phase, GSA will transition the core MPLS network to an equivalent contractor managed Layer-3 MPLS network, with security services, voice and enterprise applications. The evolution of IT services provided by the selected contractor will enable GSA to provide flexible bandwidth allocation to all GSA users. The network services acquired will be adaptable to provide services to a mobile workforce with the ability to increase and decrease bandwidth to GSA facilities according to predictive models and real-time demands.

It is GSA's intent to modernize its enterprise network in steps as a reflection of the IT services and telecommunications industry evolution. Therefore, the first service, i.e., SD-WAN may be the first modernization step adopted by GSA. The transformation to SD-WAN and other innovative approaches to IT service is expected to provide more flexibility and better cost performance over the life of the TO(s). More visibility in network platforms and their performance will allow better planning and more agile bandwidth adjustments.

C.1.3 Acquisition Approach

GSA intends to award three separate TOs, with each TO awarded to a single EIS contractor. Contractors may submit proposals for one or more task orders. The period of performance for each task order is for 13 years, starting from the date of the award. GSA reserves the right to make awards for one or multiple task orders or none at all. GSA also reserves the right to make award to one or multiple contractors or combine all three task orders and award to one contractor if it is in the government's best interest to do so.

GSA's future vision of its networking requirements are to modernize towards a highly available, secure, fully-meshed IP network that integrates all communications (voice, video, data) for both internal GSA customers as well as external customers (via a trusted internet connection). In order to accomplish this, GSA has aggregated the requirements (including MTIPS) for this modernized network into TO 1 to provide efficiencies in the management, operations, and contracting activities (see details of TO 1 services below).

Legacy voice requirements are contained in TO 2 (see details below) to streamline the voice transition, however, modern voice solutions such as IP Voice and Unified Communications will be part of TO 1. EDI VAN requirements are contained in TO 3 as they are operationally separable from the networking requirements.

Transition to EIS will involve both like-for-like and transformative elements, as GSA gradually modernizes and transforms its network architecture to meet future needs. EIS contractor(s) shall demonstrate comprehensive and proven engineering, integration and support capabilities that will assure GSA's successful implementation of new technologies and a smooth transition of services from multiple existing legacy contracts.

The scope of services for each TO is specified below. The services listed in each TO are required to be proposed by the awarded contractor(s), including the services identified as optional to buy. GSA may choose to exercise the options associated with the services identified as optional to buy, in whole or in part, based on various factors, including but not limited to, budgetary constraints and additional needs. The technical requirements for each of the services are specified in **Section C.2** of this solicitation. The GSA locations where the services and associated access arrangements required to be provided, by each TO, are specified in **Section J.1-J.3 Pricing Workbooks**.

Task Order 1 – Network

1. Required Services
   - Data
     - Ethernet Transport Service (ETS)
     - Internet Protocol Service (IPS)
     - Private Line Service (PLS)
     - Virtual Private Network Service (VPNS)
   - Managed Service
     - Managed Internet Protocol Service (MTIPS)
     - Managed Network Service (MNS)
   - Voice
     - Internet Protocol Voice Service (IPVS)
       - IPVS (VoIP)
       - Session Initiation Protocol Trunk Service
   - Access Arrangements (AA)
   - Cable and Wiring (CW)

2. Optional To Buy Services
    - Data
        - Virtual Private Network Service (VPNS)
            - Cloud Direct Connect
        - Optical Wavelength Service (OWS)
        - Dark Fiber Service (DFS)
        - Synchronous Optical Network Service (SONET)
    - Managed Service
        - Managed Network Service (MNS)
            - SD-WAN
            - Network Operations Center
            - Security Operations Center
        - Unified Communication Service (UCS)
        - Managed Security Service (MSS)
            - Palo Alto Firewall Service
    - Service Related Equipment (SRE)
    - Service Related Labor (LABOR)
    -

Task Order 2 – Voice

- Voice
    - Circuit Switched Data Service (CSDS)
    - Circuit Switched Voice Service (CSVS)
    - Toll Free Service (TFS)

The following access arrangements, SRE and labor are only to be used in conjunction with providing voice services:

- Access Arrangements (AA)
    - TDM access such as Basic Subscriber Line, BRI, and PRI
- Service Related Equipment
- Service Related Labor

Task Order 3 – Electronic Data Interchange (EDI) Value Added Network (VAN)

- Colocated Hosting Service
    - EDI VAN

C.1.4 Description of Current Environment

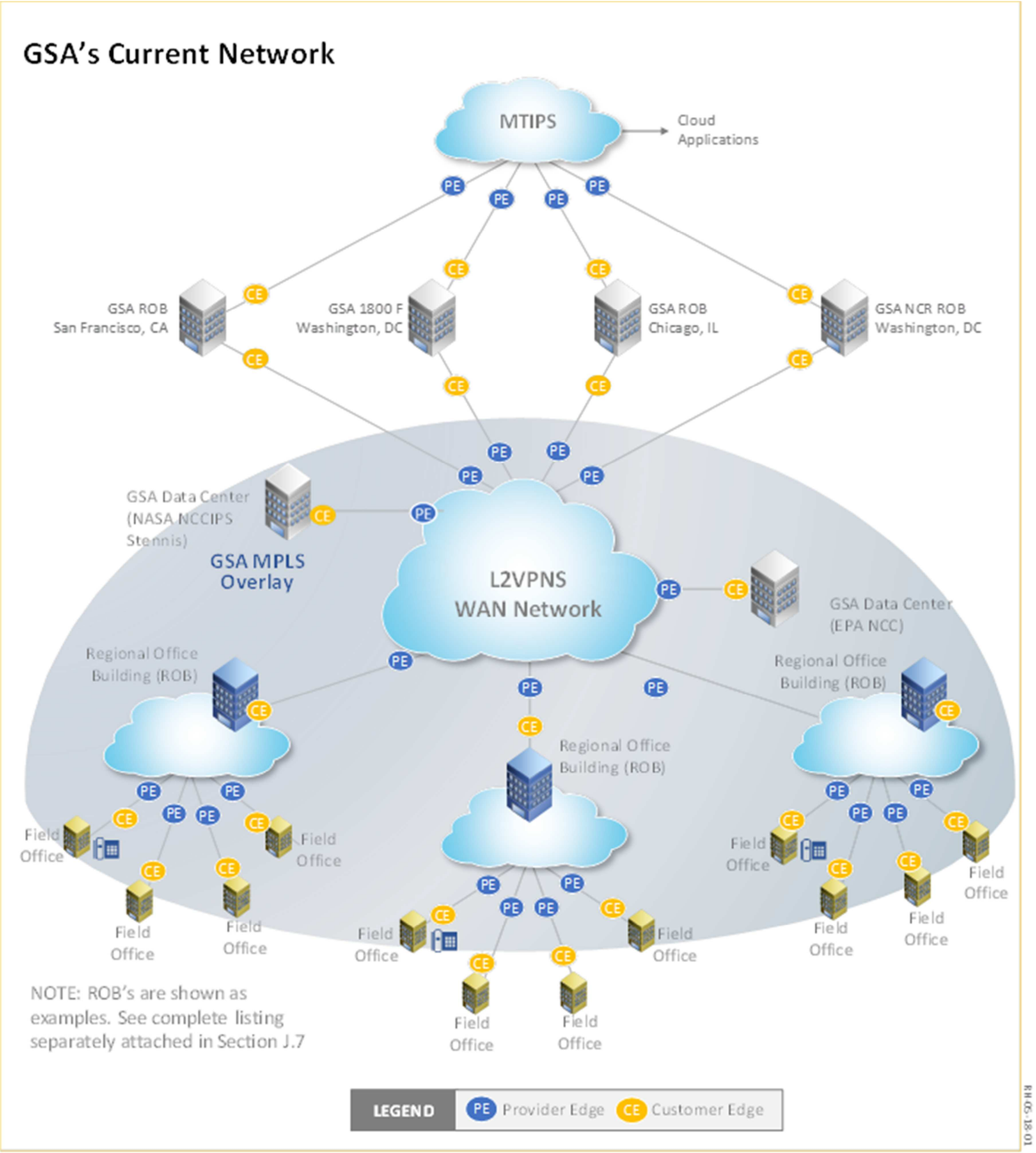
GSA's Current Network
MTIPS
Cloud Applications
GSA ROB San Francisco, CA
GSA 1800 F Washington, DC
GSA ROB Chicago, IL
GSA NCR ROB Washington, DC
GSA Data Center (NASA NCCIPS Stennis)
GSA MPLS Overlay
L2VPNS WAN Network
GSA Data Center (EPA NCC)
Regional Office Building (ROB)
Regional Office Building (ROB)
Regional Office Building (ROB)
Field Office
NOTE: ROB's are shown as examples. See complete listing separately attached in Section J.7
LEGEND
PE Provider Edge
CE Customer Edge
RHCG-18-01

Figure C-1: GSA Current Network Environment

The existing WAN is complex and has approximately 40 MPLS connections, connecting approximately 800 sites. These connections are based on a legacy hub and spoke architecture including a mixture of transport types: T1s, broadband, and managed MPLS. Many sites have T1 circuits that are bonded together (NxT1). The network infrastructure components consist of the following:

- A wide area backbone network that employs MPLS technology using Networx primary carrier for Layer-2 virtual private network (VPN) (Networx Layer-2 VPN) services to carry data traffic between the ROBs and data centers with access speeds ranging from 100 megabits per second (Mbps) to 1 gigabits per second (Gbps).
- A secondary network that uses a Networx carrier PLS with a combination of T1s and fractional T1s to connect remote FOs to the ROBs. The T1 circuits terminate on channelized DS3s using a hub and spoke architecture. The DS3s terminate on aggregation routers at the ROB locations.
- Broadband technology with varying speeds is also used at select large FOs. Broadband is being used to replace T1 circuits for the short-term.
- Internet and Intranet connectivity as well as network security to 11 ROBs, CO, several data centers, and over 800+ field sites.
- Multiple routers and/or Layer-2 switches are used to connect the LAN in the ROBs and remote FOs to the enterprise WAN.
- Internet gateways are located in DC (CO and National Capital Region (NCR)), Chicago (Region 5), and San Francisco. Each connection provides internet connectivity – 500 Mbps to 1 Gbps each. The NCR internet gateway is projected to move to the Environmental Protection Agency (EPA) National Computer Center (NCC) in Research Triangle Park, NC data center location (herein referred to as the RTP Data Center) in FY19/20 on or before this task order award.
- GSA has FOs in Europe and Asia. European locations are connected to the GSA network via the NCR site and Asian locations are connected via Region 9.
- GSA uses voice (VoIP) and video technology and has many mission essential business line applications for the Federal Acquisition Service (FAS) and Public Buildings Service (PBS) business lines.
- In 2015, GSA embarked upon modernizing its network by transitioning a subset of large FO sites (70) to a carrier managed MPLS network. Sites that were previously using bonded T1 circuits were transitioned to minimum of 10 Mbps MPLS circuit. Interconnects to the carrier's Layer-3 managed MPLS network were installed in Chicago (Region 5) and the RTP Data Center. Region 5 was selected to streamline access to the internet.

C.1.4.1 Network Node Types

The following are descriptions of each Node Type:

- Type 1: Very High Bandwidth High Availability Sites (data centers) – Used at the two GSA data centers (Stennis, MS and RTP, NC). All applications and critical services reside at GSA data centers.
  - Bandwidth shall be between 1 Gbps-10 Gbps. This may increase as the industry evolves.
  - Connectivity shall be redundant and diverse.
  - Interconnects (Raleigh (RTP), Central Office, and San Francisco (ROB), and Chicago (ROB)) shall be provisioned before other Type 2 sites (ROBs) are transitioned. These interconnects will function as critical entry points for GSA end-users to access resources residing at GSA data centers. In addition, these interconnects will provide a pathway from the current GSA managed network to the new contractor managed MPLS network. The

contractor shall work with GSA to finalize the location of these interconnects.
  - Shall include a dual path transition to SD-WAN.

- Type 2: High Bandwidth High Availability Sites (ROBs) – Primarily ROB locations and Central Office (1800 & F Street, NW Washington, DC)
  - Bandwidth shall be between 100 Mbps-1 Gbps.
  - Connectivity shall be redundant. A combination of private (MPLS) and public (e.g., broadband, 4G/5G LTE) connectivity with dynamic traffic engineering.
  - Managed SRE/MNS/universal CPE shall be capable of running various modules for future enhancements (e.g., firewall, WAN optimization etc.).
  - Use an SD-WAN architecture that is application aware and fully redundant. SD-WAN shall be architected to provide high bandwidth by aggregating disparate transport connections and shall provide automatic failover for redundancy and high-availability.
  - Shall include a dual path transition to SD-WAN.
  - An SLA shall be provided for all SD-WAN solutions.
  - The solution shall be architected, implemented and managed by the contractor.

- Type 3: Large Critical Field Office Locations – Large critical field offices that house a large number of end-users (typically 20 or more). These sites also have building management capabilities on-site.
  - Bandwidth shall be between 10 Mbps-100 Mbps for sites that currently have MPLS connections.
  - Sites with TDM connections shall be transitioned like-for-like until GSA is able to transform these sites at a later date.
  - Shall include a dual path transition to SD-WAN.
  - The contractor shall propose solutions for these sites.

- Type 4: Other Field Office Locations – Small field office locations – A standard field site with few end-users (1 to 10). These sites also have building management capabilities on-site.
  - Bandwidth shall be between 5 Mbps-30 Mbps.
  - These sites shall be transitioned like-for-like until SD-WAN technology is deployed to these sites.
  - Type 4 also includes the following types of sites with associated requirements:
    - Buildings on Military Installations – Typically serving as a Point-of-Sale/Revenue Generating Location for GSA's Federal Supply Service. Includes GSA Office of General Supplies and Services (GSS) Storefronts, GSA Enhanced Check-Out (GECO) Storefronts at Air Force, Army, Navy and Marine Corps bases and installations.
    - Border Station/Land Ports of Entry Sites – GSA’s PBS supports border stations in remote locations like Tok, Alaska. These sites

have building management capabilities and shall be on the GSA network.

- Bandwidth shall be between 5Mbps-10Mbps.

- Unstaffed Small Field Office Locations – A standard field site with no end-users. These sites support building management and Internet of Things (IoT) capabilities.
  - Bandwidth shall be 1Mbps or less.
- Commercial buildings that house a GSA-associated daycare/child care center.
- Residential locations of staff.
  - Bandwidth shall be between 1 Mbps-5 Mbps.

C.1.4.2 Voice Service

GSA currently uses a variety of technologies, such as IP Voice Service (GSA managed premises-based Cisco Unified Communication solution and Hosted VoIP), Circuit Switch Voice Service, Private Branch Exchange (PBX) service, and Toll Free Service to provide Voice services to its users throughout its locations.

C.1.4.3 Cisco Unified Communication Solution

GSA currently manages a premises-based Cisco Unified Communications solution with Public System Telephone Network (PSTN) connectivity provided via strategically located Session Initiation Protocol (SIP) Trunks. The system supports 14,000 end-users working across 250+ GSA offices and at off-site telework locations.

C.1.4.4 Building Monitoring and Control (BMC) Systems and Building Systems Network (BSN)

PBS is responsible for managing and implementing smart building technology in PBS-owned facilities. Smart Buildings are defined as specifying, planning, implementing and managing the aspects of building systems including software, protocols, networking and data, referred to as Building Monitoring and Control (BMC) Systems. BMC systems include, but are not limited to, building technologies such as advanced metering systems (AMS), building automation systems, HVAC, lighting control systems, physical access control systems (PACS) and renewable energy systems. Smart Buildings leverage technologies, data analytics and behavior to optimize buildings for operational/maintenance performance and productivity.

In order to maintain the security of the GSA network and BMC systems that reside in PBS facilities, GSA has implemented the Building Systems Network (BSN). BSN is a strategy and design concept that leverages virtual networks and access control lists (ACL) to enable logical network segmentation between building systems and the GSA ENT domain. BMC systems’ circuit needs vary based on number of users, size of building, number of connected BMC systems and its scalability for future expansion. Facilities are controlled via BMC systems. Smart building components use IoT.

PBS has a security requirement for building segmentation and isolation. GSA is required to implement a segmented BMC architecture which allows limited lateral access between buildings.

C.1.4.6 Limitations, Challenges and Constraints of the Current Environment

The limitations created by the hub and spoke network architecture and the mandate by the Office of Management and Budget (OMB) Federal Data Center Consolidation Initiative (FDCCI) to migrate servers away from GSA regional sites into the data centers have negatively impacted network services and end-user experiences at the remote locations. These conditions have led to performance and bandwidth constraints.

The following are the current operating model and constraints:

- Hub and spoke network architecture no longer satisfies end-user requirements.
- As servers migrate to the consolidated data centers, end-users experience degraded connectivity when accessing file shares and other services.
- GSA managed MPLS network is expensive and complex with multiple routing protocols and redistribution is required (i.e., Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Multiprotocol Border Gateway Protocol (MP-BGP)). Latency across the backbone is high.
- GSA FO sites have multiple T1 circuits and need to be upgraded. Bandwidth constraints impact the end-user experience.
- GSA owns all network hardware and pays maintenance on the hardware.
- The network architecture has limited failover capabilities.
- Voice/Video performance issues. Only one webcast can occur at a time. End users experience VoIP quality issues and dropped calls. Video conferences with FOs shall operate at restricted bandwidth.

C.1.5 Description of Target State Environment

GSA intends to initially transition its core MPLS network to a full mesh contractor-managed Layer-3 MPLS network, using VPNS. GSA envisions the target-state MPLS WAN to provide the following:

- "Any-to-Any" (full mesh) connectivity.
- Scalability and flexibility to respond to the evolving business needs of the agency and its stakeholders.
- Guaranteed performance levels.
- High Availability – GSA is seeking to establish a high-availability network, with automated failover, via diverse dual MPLS connections, that will be able to support mission-critical applications and services at most locations.
- High Capacity – GSA is seeking to provide high-speed network connectivity to the ROBs and FOs.
- Ubiquitous Coverage – GSA wants to ensure a consistent end-user experience regardless of physical locations (i.e., ROBs, FOs, Cloud providers, and data centers).
- Easy Scalability – GSA is seeking to increase the capacity and/or number of remote buildings serviced by the network.

- Strong Security – GSA is seeking continuous adherence to a secure network and internet connections (MTIPS).
- Smaller hardware footprint, network simplification, and a flat network topology managed by the contractor.

After the transition to the contractor managed Layer-3 MPLS network, GSA intends to eventually transform its network to a target-state hybrid SD-WAN overlay architecture solution.

C.1.6 Project Scope

The scope includes the design, engineering, provisioning, management, transition, maintenance and evolution of existing and new IT services used by GSA to support its mission.

Transitioning to EIS will address IT services required to meet the needs of GSA, as specified throughout this solicitation. The scope of the awarded TOs includes all of the current network functionality described in this solicitation, as well as those future services and capabilities offered through the EIS program that will replace or improve that functionality. In addition, the scope of the TOs include all optional and unspecified services contained in this solicitation, as well as those services required in the future to achieve GSA’s vision and needs.

The TOs will provide services to all existing GSA locations as well as any future CONUS, OCONUS, and non-domestic locations. Changes and additions of new locations will occur each year. GSA expects the contractor to provide service without interruption.

C.1.7 Transition Approach

A high-level transition approach, for each task order, to EIS is described below. The estimated transition and transformation timeline for each service, during the task orders 13 year period of performance are reflected in **Section J.1-J.3 Pricing Workbooks**.

C.1.7.1 Task Order 1 – Network

The transition to EIS and transformation of the GSA network infrastructure and services shall occur in a phased approach. The primary objective of this task order is to initially transition the core network infrastructure and services to EIS, prior to the expiration of the legacy GSA contracts (i.e., Networx, WITS 3, LSAs). This will be followed by the modernization and transformation phase, which may include implementing some of the optional to buy services. The modernization and transformation of services will occur throughout the task order period of performance.

The estimated transition and transformation timelines, for the services in this TO, are reflected in **Section J.1Pricing Workbook: TO 1**.

The following describes the suggested initial transition and transformation phases of specific services.

C.1.7.1.1 Initial Transition Phase:

1. **Network Infrastructure**
    - o Transform the GSA managed Layer-2 MPLS network to a fully meshed and fully managed Layer-3 MPLS network.
        - ▪ ROBs, data centers and a select number large FOs shall be transitioned to the fully managed MPLS network, while other sites (FOs, European sites and MTIPS) will transition like-for-like.
        - ▪ Transition all connections (MPLS, ETS, PLS, Broadband (IPS), Wireless (4G/LTE)) like-for-like for all node types, as specified in **Section C.1.3** of this solicitation.
        - ▪ Implement WAN Optimization as part of the managed MPLS service.
    - o Transition all existing contractor managed Layer-3 MPLS connections like-for-like.

2. **MTIPS**
    - o Transition the four Internet connections at the MTIPS sites like-for-like.

3. **Voice**
    - o Transition geographically diverse SIP Trunks like-for-like to support off-net calling to the PSTN.

C.1.7.1.2 Transformation Phase:

This phase shall be implemented throughout the period of performance to modernize and consolidate the following infrastructure and services:

1. **Network Infrastructure**
    - o Transform to the hybrid SD-WAN overlay architecture solution
        - ▪ Transform all TDM T1 connections at the FOs to either Ethernet or Broadband connections, for node types specified in **Section C.1.3** of this solicitation, to increase WAN capacity and scalability.
        - ▪ Transform all TDM T1 connections at sites managed by the Building Management Systems (BMS) to either Ethernet or Broadband connections, for node types specified in **Section C.1.3** of this solicitation, to increase WAN capacity and scalability and incorporate the Building System Network (BSN) as part of the SD-WAN transformation.

2. **MTIPS**
    - o Consolidate the Internet connections at the MTIPS sites from 4 to 3 or 2.
        - ▪ The connections shall be geographically diverse – one on the East Coast and one on the West Coast. The internet connections shall be architected for stateful failover.

3. **Security**
    - o Transition perimeter Demilitarized Zone (DMZ) firewalls at the MTIPS sites to a contractor hosted and managed security solution.

- Transition the GSA managed Palo Alto firewall to a contractor hosted and managed Palo Alto security solution.
- Transform to a contractor managed 24/7 SOC monitoring service.

4. **Managed Network Services**
   - Implement a contractor managed NOC service.
   - Implement a contractor managed 24/7 SOC monitoring service.

5. **Voice**
   - **TDM Voice**
     - Transform TDM voice services to functional equivalent IP-based voice services.
   - **Cisco Unified Communications Manager (CUCM) VoIP**
     - Transform GSA managed premises-based CUCM VoIP platform to a contractor managed hosted UCS VoIP solution.

C.1.7.2 Task Order 2 – Voice

The objective of this task order is to transition all TDM voice services to EIS by the required due date, prior to the expiration of GSA legacy services. This objective is presented primarily due to implied market conditions of the potential downturn of TDM-based services. However if contractors provide stable, reliable, and economically feasible services through the life of the task order there may be less need to transition unless the migration to IP-based voice services provides better value to the government.

There's an expectation that the legacy CSVS circuits will reduce over time, but GSA does not know when these circuits will be disconnected. Also, it is expected that the TFS volume will stay relatively flat throughout the task order period of performance.

1. **TDM Voice**
   - Transition all analog lines, ISDN BRIs and ISDN PRIs like-for-like.
   - Transition CSDS access circuits and service like-for-like.
   - Transition TFS like-for-like.

C.1.7.3 Task Order 3 – Electronic Data Interchange (EDI) Value Added Network (VAN)

GSA currently uses a commercial, non-custom EDI VAN service (e.g., Advanced Communications Systems (ACS), CovalentWorks, IBM Sterling, Kleinschmidt, Simplix, TrueCommerce), as a custom Colocated Hosting solution on the Networx contract. The business-to-business (B2B) service allows GSA to interconnect with its trading partners to send/receive transactions and exchange electronic files.

GSA is seeking to transition to an equivalent custom Colocated Hosting solution on EIS; however the EDI VAN service itself is a commercial, non-custom solution that provides a secure, comprehensive hosted electronic data collaboration solution which provides GSA and its trading partners with advanced data exchange and systems integration, visibility into key business document process management, simplified partner on-boarding and management processes, and end-to-end business process management.

C.1.8 Alternative Approach

Contractors may also include additional, alternative solutions that provide comparable or better performance in innovative ways. Proposals with alternative approaches should contain a detailed description of the solution including a Performance Work Statement (PWS) and pricing that uses fixed price CLINs, whenever possible.

Note that alternative approaches will only be accepted for the TO 1 and TO 3 required services. For TO 3, contractors may propose alternative pricing structures for the requirements specified in **Section C.2.3.1** of this solicitation. No alternative approaches shall be proposed for TO 2.

C.2 Technical Requirements

GSA requires the provision of EIS services to meet the needs stated in this section. Contractors shall propose services as defined below to meet these needs.

The contractor shall propose services that meet the requirements described in the section for the services in the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.1 Data Service

C.2.1.1 Virtual Private Network Service (VPNS)

The contractor's VPNS solution shall meet the requirements described in **Section C.2.1.1** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

The VPNS solution shall support IPv4 and IPv6 interoperability and the eventual transition from IPv4 to IPv6 in the future.

C.2.1.1.1 Cloud Direct Connect – Optional to Buy

The contractor shall provide the ability to directly and securely interconnect with major CSPs, such as AWS, Google Cloud Platform and Microsoft Azure, via the VPNS backbone without requiring a separate circuit to the CSP. The service shall include only the transport without the management of the Virtual Private Cloud (VPC).

Connectivity through the TIC for DHS-mandated internet-facing applications shall not be required.

GSA currently connects to the AWS, from its data centers, using VPN tunnels over the Internet.

C.2.1.1.2 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.1.1.1.3 Connectivity** within the VPNS section in the EIS contract.

C.2.1.1.3 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.1.1.1.4 Technical Capabilities** with the VPNS section of the EIS contract.

C.2.1.1.4 Features

The contractor's solution shall provide the features described in **Section C.2.1.1.2 Features** within the VPNS section of the EIS contract, including ID #2 Interworking Services.

C.2.1.1.5 Performance Metrics

The contractor's VPNS solution shall meet the performance levels as specified in **Section C.2.1.1.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs** of the EIS contract.

C.2.1.2 Ethernet Transport Service (ETS)

GSA requires ETS. The contractor's ETS solution shall meet the requirements described in **Section C.2.1.2 Ethernet Transport Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.1.2.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.1.2.1.3 Connectivity** within the ETS section in the EIS contract.

C.2.1.2.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.1.2.1.4 Technical Capabilities** within the ETS section of the EIS contract.

C.2.1.2.3 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in ETS **Section C.2.1.2.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.1.3 Optical Wavelength Service (OWS) – Optional to Buy

The contractor's OWS solution shall meet the requirements described in **Section C.2.1.3 Optical Wavelength Service** of the EIS contract.

C.2.1.3.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.1.3.1.3 Connectivity** within the OWS section in the EIS contract.

C.2.1.3.2 Technical Capabilities

The contractor’s solution shall include the technical capabilities as described in **Section C.2.1.3.1.4 Technical Capabilities** within the OWS section of the EIS contract.

C.2.1.3.3 Features

The contractor’s solution shall provide features as described in **Section C.2.1.3.2 Features** within the OWS section of the EIS contract.

C.2.1.3.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in **Section C.2.1.3.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs** of the EIS contract.

C.2.1.4 Private Line Service (PLS)

The contractor's PLS solution shall meet the requirements described in **Section C.2.1.4 Private Line Service** of the EIS contract.

C.2.1.4.1 Connectivity

The contractor's solution shall meet the connectivity requirements described in **Section C.2.1.4.1.3 Connectivity** within the PLS section in the EIS contract.

C.2.1.4.2 Technical Capabilities

The contractor’s solution shall include the technical capabilities as described in **Section C.2.1.4.1.4 Technical Capabilities** within the PLS section of the EIS contract.

C.2.1.4.3 Features

The contractor’s solution shall provide the features described in **Section C.2.1.4.2 Features** within the PLS section of the EIS contract.

C.2.1.4.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in PLS **Section C.2.1.4.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.1.5 Synchronous Optical Network Service (SONETS) – Optional to Buy

The contractor's (SONETS) solution shall meet the requirements described in **Section C.2.1.5 Synchronous Optical Network Service** of the EIS contract.

C.2.1.5.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.1.5.1.3 Connectivity** within the SONETS section in the EIS contract.

C.2.1.5.2 Technical Capabilities

The contractor’s solution shall include the technical capabilities as described in **Section C.2.1.5.1.4 Technical Capabilities** within the SONETS section of the EIS contract.

C.2.1.5.3 Features

The contractor’s solution shall provide features as described in **Section C.2.1.5.2 Features** within the SONETS section of the EIS contract.

C.2.1.5.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in SONETS **Section C.2.1.5.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.1.6 Dark Fiber Service (DFS) – Optional to Buy

GSA requires DFS. The contractor’s DFS solution shall meet the requirements described in **Section C.2.1.6 Dark Fiber Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.1.6.1 Connectivity

The contractor's solution shall meet the connectivity requirements as explained in **Section C.2.1.6.1.2 Connectivity** within the DFS section in the EIS contract.

C.2.1.6.2 Technical Capabilities

The contractor’s solution shall include the technical capabilities as described in **Section C.2.1.6.1.4 Technical Capabilities** within the DFS section of the EIS contract.

- The contractor shall provide a DFS solution to support the locations specified in **Section J.1 Pricing Workbook**.
- The contractor shall provide access path diversity and access path avoidance arrangements at sites specified in **Section J.1 Pricing Workbook** of this solicitation.

C.2.1.6.2 Features

The contractor’s solution shall provide features described in **Section C.2.1.6.2 Features** within the DFS section of the EIS contract.

GSA location-specific dependencies of the above DFS features can be found in **Section J.1 Pricing Workbook** of this solicitation.

C.2.1.6.2 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in DFS **Section C.2.1.6.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs.**

C.2.1.7 Internet Protocol Service (IPS)

The contractor's IPS solution shall meet the requirements described in **Section C.2.1.7 Internet Protocol Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.1.7.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.1.7.1.3 Connectivity** within the IPS section in the EIS contract.

C.2.1.7.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.1.7.1.4 Technical Capabilities** within the IPS section of the EIS contract.

C.2.1.7.3 Features

The contractor's solution shall include the features in the table below. These features are described in **Section C.2.1.7.2 Features** within the IPS section of the EIS contract.

Table C-1 Internet Protocol Service Features

Name of IPS Feature	Custom Requirements
Class of Service (CoS)	The contractor shall accommodate and optimize an agency's applications to enable the network to accurately and consistently allow for traffic prioritization and cost-efficiencies. The Classes of Service or prioritization levels may be categorized as: 1. Premium for time-critical traffic such as voice and video 2. Enhanced for business-critical traffic such as transactions 3. Standard for non-critical traffic such as email.

C.2.1.7.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in IPS **Section C.2.1.7.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.1.8 High-Speed Data Connection Solutions

GSA has a requirement for highly secured and highly available connections between its data centers (Node Type 1). The connections are optional to buy.

Currently, GSA provides connectivity between its data centers using a Networx 1 Gbps L2VPNS circuit.

The contractor shall propose a functional equivalent solution for 1 Gbps dual path connections, using one of the following EIS services: VPNS, OWS, SONETS or DFS. The proposed solution shall not require any special construction. **Section J.1 Pricing Workbook Tab 4** identifies the sites where the high-speed data connection solutions are required and provides additional submission instructions.

C.2.2 Voice Service

C.2.2.1 Internet Protocol Voice Service (IPVS)

The contractor's IPVS solution shall meet the requirements described in **Section C.2.2.1 Internet Protocol Voice Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.2.1.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.2.1.1.3 Connectivity** within the IPVS section in the EIS contract.

C.2.2.1.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.2.1.1.4 Technical Capabilities** within the IPVS section of the EIS contract.

- Number Portability – The contractor shall port all the existing telephone numbers when transitioning to EIS.
- Uniform Dialing Plan
  - The contractor shall provide a uniform dialing plan for all users across the GSA voice network.
  - The contractor shall provide a single point of administration and maintenance of the dialing plan.
- Softphone Client – The contractor shall provide softphone clients as part of the solution and shall be able to integrate with the existing GSA directory and identity manager infrastructure.
- System Diagnostic and Alarms – The contractor shall provide integrated diagnostic capabilities and alarms inherent within the system for routine system monitoring, remote diagnostics, and remote repair capabilities.
- Failover to the PSTN – The contractor shall include failover capabilities that support call resiliency for all GSA locations that support diverse SIP trunks at diverse SDPs. The solution shall provide the VoIP network with the ability to failover to the PSTN, via the CSVS solution, if available.

C.2.2.1.3 Features

The contractor's solution shall provide the features as described in **Section C.2.2.1.2 Features** within the IPVS section of the EIS contract.

C.2.2.1.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in IPVS **Section C.2.2.1.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.2.1.5 Managed LAN Service – Cat 3 Wiring

The contractor shall support reusing of existing telephony wiring consisting of 24 AWG twisted pair or 26 AWG twisted pair as part of the Hosted or Premises-Based Managed LAN solution. The contractor shall provide TO unique "Hosted Managed LAN Service – Cat 3 Wiring Reuse" and "Premises-Based LAN Service – Cat 3 Wiring Reuse" solutions which include the use of terminal adapters allowing support of IP/SIP Phones (Class 2 IEEE 802.3af compliant) with existing telephony wiring.

C.2.2.2 Circuit Switched Voice Service (CSVS)

The contractor's CSVS solution shall meet the requirements described in **Section C.2.2.2 Circuit Switched Voice Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.2.2.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.2.2.1.3 Connectivity** within the CSVS section in the EIS contract.

C.2.2.2.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.2.2.1.4 Technical Capabilities** within the CSVS section of the EIS contract.

- Number Portability – The contractor shall port all the existing telephone numbers when transitioning to EIS.
- Uniform Dialing Plan
    - The contractor shall provide a uniform dialing plan for all users across the GSA voice network.
    - The contractor shall provide a single point of administration and maintenance of the dialing plan.

The contractor shall support the following user-to-network interfaces at the SDP:

- **ISDN PRI trunk (23 B + D):** An information-payload data rate of 1.472 Mb/s and ITU-TSS Q.931 signaling type. D channel cannot be shared by another ISDN PRI trunk. (Standards: ANSI/EIA T1.607 and 610; NIUF National ISDN-1 [Bellcore Pub SR-NWT-001937], NIUF National ISDN-2 [Bellcore Pub SR-NWT-002120], and NIUF National ISDN-3 [Bellcore Pub SR-NWT-002457].)
- **ISDN PRI trunk (24 B + 0 D):** An information-payload data rate of 1.536 Mb/s and ITU-TSS Q.931 signaling type. Shares a D channel with another PRI trunk. (Standards: ANSI/EIAT1.607 and 610; NIUF National ISDN-1 [Bellcore Pub SR-

NWT-001937], NIUF National ISDN-2 [Bellcore Pub SR-NWT-002120], and NIUF National ISDN-3 [Bellcore Pub SR-NWT-002457].)

- **ISDN PRI trunk (23 B + D):** An information-payload data rate of 1.472 Mb/s and ITU-TSS Q.931 signaling type. D channel can be shared with a maximum of 10 ISDN PRI trunks. (Standards: ANSI/EIA T1.607 and 610; NIUF National ISDN-1 [Bellcore Pub SR-NWT-001937], NIUF National ISDN-2 [Bellcore Pub SR-NWT-002120], and NIUF National ISDN-3 [Bellcore Pub SR-NWT-002457].)

C.2.2.2.3 Features

The contractor's solution shall provide features as described in **Section C.2.2.2.2** within the CSVS section of the EIS contract.

C.2.2.2.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in **Section C.2.2.2.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs** of the EIS contract.

C.2.2.2.5 Local Dial Tone Unlimited Calling Plan

The contractor shall provide TO unique unlimited local calling plans that unbundle local calling, long distance and features for analog voice lines, ISDN PRI trunks, and ISDN BRI lines. The local calling area shall include the local exchange area and all areas within the same LATA (IntraLATA). The dial tone unlimited calling plans shall include:

- Unlimited on-net to on-net and unlimited CONUS on-net to CONUS off-net local calling.
- Unlimited off-net local calling within the same OCONUS county/jurisdiction, for service implementations located in an OCONUS country/jurisdiction.
- On-net to off-net long distance calls will be charged per usage according to **Section B.2.2.2.1.2** of the EIS contract.

C.2.2.3 Toll Free Service (TFS)

The contractor's TFS solution shall meet the requirements described in **Section C.2.2.3 Toll Free Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.2.3.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.2.3.1.3 Connectivity** within the TFS section in the EIS contract.

C.2.2.3.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.2.3.1.4 Technical Capabilities** within the TFS section of the EIS contract.

- The contractor shall support number portability and shall transition all GSA existing toll free telephone numbers to EIS with minimal disruption and interference.
- The contractor shall ensure toll free service can provide ANI and Dialed Number Identification Service (DNIS) in accordance with **Section C.2.2.3.2** of the EIS contract.

C.2.2.3.3 Features

The contractor's solution shall include the features as described in **Section C.2.2.3.2** within the TFS section of the EIS contract.

- The contractor shall make toll free numbers accessible from CONUS, OCONUS, and Canada when requested by GSA.
- The contractor shall utilize standard North American numbering plan.
- The contractor shall provide the ability to configure Time of Day, Day of Week, and federal holiday routing.
- The contractor shall provide the ability to configure Alternate Routing Plans.
- The contractor shall provide 24/7 helpdesk support to implement routing plan changes and percent allocations or provide self-administration capabilities to allow GSA to perform the required updates.
- The contractor shall provide the ability to block all calls originating from pay phones.
- The contractor shall provide the ability to record audio announcements remotely, via a contractor provided dial-in number.

C.2.2.3.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in TFS **Section C.2.2.3.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.2.4 Circuit Switched Data Service (CSDS)

The contractor's CSDS solution shall meet the requirements described in **Section C.2.2.4 Circuit Switched Data Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.2.4.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.2.4.1.3 Connectivity** within the CSDS section in the EIS contract.

C.2.2.4.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.2.4.1.4 Technical Capabilities** within the CSDS section of the EIS contract.

C.2.2.4.3 Features

The contractor’s solution shall include the features as described in **Section C.2.2.4.2 Features** within the CSDS section of the EIS contract.

C.2.2.4.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in CSDS **Section C.2.2.4.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.3 Collocated Hosting Service (CHS)

The contractor’s CHS solution shall meet the requirements described in **Section C.2.4 Colocated Hosting Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.3.1 Electronic Data Interchange Value Added Network (EDI VAN)

The commercial, non-custom EDI VAN solution shall provide:

- Protocol Interface:
  - CSDS (FTP/SFTP), IPS (HTTPS), VPNS, and Application Standard 2 (AS2).
- Security:
  - Support AS2 security protocol and digital certificates.
  - Commercial best security practices shall be used to securely protect the transaction data stored on the VAN platform.
- Usage:
  - Unlimited EDI data usage and not metered per kilo-character shall be part of the service.
- Storage:
  - Unlimited storage capacity of the transaction data between GSA and its trading partners.
  - The transaction data shall be stored, for online access by GSA, on the VAN platform at a minimum of 30 days.
- Translation:
  - Does not require data translation functionality as part of the transaction communication.
  - Provide functional equivalent desktop translation software as the Sterling Integrator B2B 5.25 software, which GSA currently uses to perform its own data translation.
  - Support ANSI X.12 data format.
- SLAs:
  - The Performance Metrics shall meet the requirements described in **Section C.2.4.5.1 Performance Metrics** of the EIS contract.
- Online Portal

  - Web-based dashboard/portal to conduct daily business, which includes trading partner support such as onboarding, transaction queries, re-queuing transactions, etc.
- Help Desk Support:
  - A customer service 800 number to report issues and/or assist with problem resolution.
- Easy ramp-on process for trading partners.
- Exchange with trading partners directly or via their own VAN (interconnections with other VANs).
- Provide assistance with the transition, which includes, but not limited to, notifying trading partners of the impending transition to the new VAN platform and provide any additional necessary information to interconnect with GSA on the new VAN platform.
- Provide the flexibility to allow GSA to transform to a new EDI service in the future in order to take advantage of innovative technologies, such as IBM Blockchain.

The contractor shall provide the following deliverables:

- Monthly Status Report to include new trading partners added, transaction volume, and a summarized list of transactions per contractor (both inbound and outbound).
- Transition Plan to include a communication to existing trading partners about transitioning to a new VAN. The plan shall also include details to include the frequency of the communication to non-responsive contractors.
- Set up and testing of the new communications link with the new VAN.
- VAN point of contact list.

C.2.4 Managed Service

C.2.4.1 Managed Network Service (MNS)

The contractor's MNS solution shall meet the requirements described in **Section C.2.8.1 Managed Network Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

The contractor shall take over and provide full management of the WAN GFE, as a feature of EIS MNS. This shall include providing ongoing monitoring, maintenance, upgrade, and management of all the components of the GFE.

The GFEs shall be initially assessed to meet the requirements to be managed by the contractor. In cases where the hardware is not certified to be managed or a refresh is required, the contractor shall provide the updated hardware and required software as an SRE monthly recurring plan.

C.2.4.1.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.8.1.1.3 Connectivity** within the MNS section in the EIS contract.

C.2.4.1.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.8.1.1.4 Technical Capabilities** within the MNS section of the EIS contract.

MNS shall enable GSA to obtain design and engineering, implementation, management, and maintenance services for the GSA's network enterprise. Details of the tasking will be described by the government in the individual service order, which may include, but not be limited to, the following:

- Design and Engineering Services (See **Section C.2.8.1.1.4.1** of the EIS contract).
- Implementation, Management, and Maintenance (See **Section C.2.8.1.1.4.2** of the EIS contract).
    - Access solutions that use a combination of different services.
    - Transport solutions that distribute traffic over multiple contractor backbone networks to provide redundancy and diversity.
    - Customer premises solutions that provide agency-specific interfaces, software, and equipment.
    - Security solutions as required by the agency.

The contractor shall provide the necessary technical and operational capabilities to ensure the availability and reliability of GSA's network infrastructure and systems.

C.2.4.1.3 Features

The contractor's solution shall include the features in the table below. These features are described in **Section C.2.8.1.2 Features** within the MNS section of the EIS contract.

Table C-2 Managed Network Service Features

Name of MNS Feature	Custom Requirements
GFP and GFE Maintenance	The contractor shall maintain and repair GFP and GFE.
Agency-Specific NOC and SOC	Agency-Specific NOC and SOC. The contractor shall provide agency-specific help desk services and shared or dedicated NOCs and SOCs to meet agency requirements.
Network Testing	Network Testing. The contractor shall support agency-specific development services which address the agency's potential need to test equipment, software and applications on the contractor's network prior to purchase and deployment. This shall cover voice, data, and video technologies that include but are not limited to IP VPN and voice services. Testing shall be performed at the agency's discretion and structured in collaboration with the contractor.
Traffic Aggregation Service (DHS)	Traffic Aggregation Service (DHS Only). The contractor shall establish and maintain secure facilities ("DHS EINSTEIN Enclaves") where DHS-furnished equipment can be deployed, provide network connectivity from the DHS EINSTEIN Enclave to the DHS data centers, and route all traffic subject to National Policy requirements described in **Section C.1.8.8 National Policy Requirements** of the EIS contract through (i.e., deliver to and receive from) a DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. Once traffic is received at the EINSTEIN Enclave and processed, it is sent back to the contractor for delivery to its destination. The contractor shall assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communications links, and shall provide engineering support to integrate the DHS GFP sensor

	equipment, data center and communications infrastructure into the contractor's services. The contractor shall assist DHS in the maintenance and repair of the sensor system to the extent of receiving phone calls or emails requesting "Smart-Hands" service of DHS-supplied equipment.

C.2.4.1.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in MNS **Section C.2.8.1.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.4.1.5 Network Operations Center (NOC) – Optional to Buy

The contractor shall provide shared tier 1, 2 and some tier 3 Network Operations support for all GSA networking components. The contractor's NOC shall interact with the GSA NOC to provide seamless problem resolution.

Contractor support shall include, but is not limited, to the following:

- Monitoring Support – Monitoring, operations and management of all physical and logical layer connections and configurations.
- Fault Management – Discovery and recovery of problems within the network, including fault detection, isolation, correlation, and recovery.
- Configuration Management – Management of hardware and software configurations for all components that make up the contractor's network. This includes the understanding of how each device interacts within the network and how the device is configured.
- Capacity Management – The contractor shall provide monthly resource usage and utilization reports or have this information available via a portal.
- Performance Management – The contractor shall gather network statistics, and evaluate network performance over time. This includes, but is not limited, to providing metrics for QOS and SLAs.

The contractor shall have their shared NOC and the associated managed network services to operate and manage their backbone network services and circuits as required by the EIS contract. The contractor's shared NOC/Network Management System (NMS) shall work closely to coordinate all its activities with the GSA NOC.

The contractor shall also provide other associated services such as, but not limited to, program, design, engineering, integration testing and transition support. See table below for management areas.

Table C-3 Management Areas

Network Component	Contractor Shared NOC/NMS and Field Support Functions	GSA NOC/NMS Functions	LEC Functions
Enterprise Level	End-to-end view of network, Summary Reports on Performance/SLAs, Resource	Contractor to provide required information to GSA/NOC to support Enterprise Level	

	Utilization, Capacity Bottlenecks	Management. SLAs, Reports, bandwidth utilization, trouble summary, etc. on GSA access and backbone. Integration of information from all other areas to allow intelligent monitoring.	
GSA Node Level	Monitoring, Fault management, Performance management, Configuration Control/Change Management, Implementation Management, Remote Diagnostics, Issuing trouble ticket for maintenance/repair, Utilization/Reports. Provision, Installation/De-installation, Implementation, Maintenance, Repair, Add/Moves, Upgrade. Security upgrades and vulnerability remediation.	Contractor to coordinate tasks with GSA NOC for seamless impact to GSA end-users.	
Access Level	Monitoring through CPE interface, Indirect monitoring through Service Provider NOC/NMS, issuing Trouble ticket, Utilization Measure/Traffic trending. Monitoring, Maintenance, Repair (own access), Issuing trouble ticket to LEC, Coordinate with LEC installation/de-installation, Utilization Measure/Traffic trending, Status/performance coordination with GSA NOC.	Coordination and cooperation with contractor NOC to resolve network faults and other issues. SNMP read-only access to devices deployed within GSA network.	Monitoring, Maintenance, Repair, Upgrade, Installation/ De-installation, Status feed to Service Provider on access status.
POP	Near real-time status and visibility through contractor's NOC. Monitoring, Maintenance, Repair, Upgrade, Management, Status/ performance feed to GSA NOC.	Coordination and cooperation with Service Provider's NOC to resolve network faults.	
POP to Provider Customer Edge (CE) Router	Near real-time status and visibility through Service Provider NOC/NMS. Monitoring, Maintenance, Repair, Upgrade, Traffic management, Status/ performance feed to GSA NOC.	Coordination and cooperation with Service Provider's NOC to resolve network faults.	

Core (IP MPLS; NB IP VPN) Backbone	Status and visibility through contractor's NOC/NMS. Monitoring, Maintenance, Repair, Upgrade, Traffic management, Status/ performance.	Coordination and cooperation with Service Provider's NOC to resolve network faults. SNMP read-only access to devices deployed within GSA network.	
Security	Near real time netflow feed to GSA security appliances.		

C.2.4.1.6 Security Operations Center (SOC) – Optional to Buy

The 24/7 (24 hours/day, 7 days/week) SOC monitoring solution service shall provide the following:

- Monitor events from servers, laptops, network devices and security tools, and notify GSA about suspected compromise or impending compromise within 15 minutes of initial detection.
- Directly monitor GSA's existing SIEM tool and correlate events from the SIEM raw event feed.
- The contractor is expected to know GSA's infrastructure well enough to distinguish between a random intrusion attempt and a successful intrusion. GSA is not interested in calls about routine portscans and probing. (See next bullet about preventative action) GSA requests information on events that can't be blocked, need manual intervention and/or require activating the incident response team.
- Take independent preventative action to block malicious activity at the perimeter or using existing security tools (application whitelisting, etc.). Scenarios for automatic blocking will be agreed upon in advance.
- Support/process an estimated event rate of:
  - 3-4 Billion events per day
  - 3-4 Terabytes of data per day
- Support/monitor 400 web accessible servers, 18,000 laptops, and 30,000-40,000 total devices on and off network.
- Address and resolve the expected 20-30 daily correlated actionable events.

C.2.4.2 Unified Communications Service (UCS) – Optional to Buy

The fully managed hosted UCS solution shall integrate seamlessly all the key components (i.e., VoIP, email, instant messaging, unified messaging, presence, audio and web conferencing, calendar, and desktop sharing) required for a robust enterprise-wide communications and collaboration platform. The solution shall support integration with external application suites (e.g., Google collaboration suites, Adobe Connect) and accessible to the UCS services using VMware Horizon (Virtual Desktop Application) and client based VPN applications.

The contractor shall provide an enterprise UCS solution and strategy for transformation that will provide "anywhere, anytime, on any device" collaboration platform. The UCS solution shall support interfaces such as IP/SIP phones, softphones, mobile phones, web browsers, email clients, desktop clients, PCs and tablets.

The transformation to the contractor managed UCS platform shall occur in phases in order to minimize disruption to the end-users. Initially, transforming the GSA managed CUCS VoIP solution then followed by transforming the conferencing, collaboration tools and integration with external applications.

The following UCS and VoIP requirements through a FedRAMP authorized cloud-hosted solution shall be supported.

Table C-4 UC and VoIP Requirements

General User Requirements
○ A unique phone number. ○ A voice mailbox. ○ Number portability. ○ Local and long distance calling capabilities. ○ A mobile client for smartphone (WIFI calling). ○ Softphone on laptops or computers. ○ E-911 support with dynamic location tracking of desk phones and softphones at GSA office locations and possibly home or alternative remote locations (currently Cisco 79XX series phones, Cisco Jabber, Cisco 88XX conference room phones). ○ Single Number Reach. ○ Video conferencing capability (currently Adobe Connect / Cisco CMS / Cisco Jabber / SIP and H.323 Video end-points). ○ Web and audio conferencing (currently Adobe Connect / Cisco CMS / Cisco Codian). ○ Access to agency phone directory. ○ H.323, SIP and H.320 interoperability. ○ IPv4 and IPv6 interoperability.
Specific Users / Locations / Phone Line Requirements
○ International calling capabilities, with permission from a supervisor. ○ A multi-line display phone with speakerphone and message waiting indicator (for personal lines and shared office line(s). ○ Access to shared office line and voicemail. ○ 508 Compliant Telephone Devices (such as IP Blue softphone, Video Phone etc.). ○ Access to ACD like functionality. ○ Access to Call Center functionality (currently UCCX) with 20 licenses. ○ E-fax integration with email (currently Esker and Gmail). ○ A physical conference room phone(s) with extension microphones. ○ Building Paging (currently Cistera). ○ VTC (video teleconference) Interoperability (currently Integration with 3rd party SIP devices such as Bi-AMP, Polycom, ClearOne cards which connect VoIP to VTC rooms). ○ Support for SIP voice trunks to third party servers and devices. ○ Published Numbers (when requested). ○ Support for Telepresence end-point registration (currently Cisco Telepresence with Cisco Unified Communications Manager - CUCM, Tandberg Management Suite-TMS and Video Communication Server - VCS). ○ Support for Telepresence conferences (currently Cisco Codian Multipoint Control Units - MCUs). ○ Conference scheduling and Virtual Meeting Room support (currently Cisco TMS for scheduling).

The contractor's Unified Communications Service solution shall meet the requirements described in **Section C.2.8.3 Unified Communications Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.4.2.1 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.8.3.1.3 Connectivity** within the Unified Communications Service section in the EIS contract.

C.2.4.2.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.8.3.1.4 Technical Capabilities** within the Unified Communications Service section of the EIS contract.

- The hosted UCS platform shall meet FedRAMP moderate level specifications.
- The contractor shall assess GSA's IP Voice network infrastructure and capacity to support and integrate with the hosted UCS platform.
- The UCS shall be able to interoperate with IP Voice and TDM Voice services, using appropriate TDM-IP gateways/bridges to the UCS IP platform.
- The UCS shall interoperate with other communications and conferencing systems utilized by GSA. The contractor shall configure UCS interconnection and interoperability with the enterprise voice systems at all GSA locations identified in **Section J.1 Pricing Workbook**.
- The contractor shall provide the necessary technical and operational capabilities to ensure the availability and reliability of the UCS platform.
- The contractor shall provide online self-training guides on how to use the UCS services on all supported interface devices.
- The contractor shall provide real-time proactive monitoring, rapid troubleshooting and service restoration. This includes providing support services to the GSA IT organization to troubleshoot any performance or outage related issues.

C.2.4.2.3 Features

The contractor's solution shall include the features described in **Section C.2.8.3.2 Features** within the Unified Communications Service section of the EIS contract.

C.2.4.2.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in Unified Communications Service **Section C.2.8.3.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.4.3 Managed Trusted Internet Protocol Service (MTIPS)

GSA has a requirement for the contractor to provide the capability for a secured connectivity to the public internet using the Managed Trusted Internet Protocol Service (MTIPS). The contractor shall deliver and support MTIPS which shall comprise two (2) parts: (1) TIC Portal (TIC Access Points) and (2) Transport Collection and Distribution (MTIPS Transport).

GSA currently has 4 MTIPs connections located at the following sites:

- Washington, DC: 1800 F Street, NW, Washington, DC
- National Capital Region[1] (NCR): 301 7th Street, SW, Washington, DC
- Chicago (Region 5): 230 South Dearborn Street, Chicago, IL
- San Francisco (Region 9): 50 United Nations Plaza, San Francisco, CA

Each connection provides internet connectivity between 700 Mbps to 1 Gbps.

The contractor shall:

- Transition the current MTIPs Internet connections that are TIC compliant like-for-like.
- Natively route the existing American Registry for Internet Numbers (ARIN) allocation of the IPV4 Class B network 159.142.0.0/16. In addition, GSA requires IPV4 native routing for four (4) Class C networks in direct allocation from ARIN, which are: 192.149.11.0/24,192.136.12.0/24,198.177.227.0/24, and 206.137.126.0/24.
- Provide Network Address Translation (NAT) services to provide internet access for Class C networks that are part of the GSA Private Address Space (RFC 1918). This will require the contractor to furnish sufficient public address space to cover these private networks. GSA requires that the contractor provide simple Network Address Translation, or Port Address Translation (Overloading/Hiding) but will not accept application proxy as a solution.
- Comply with the IPv6 OMB mandate, GSA requires that the following IPV6 network (Direct ARIN allocation) 2620:0:150::/48: is supported and routed by the MTIPS contractor.
- Deliver a machine readable log stream to GSA that includes medium, high and critical severity alerts/threats/events in real time (no more than 30 minutes) of the generation of these alerts/threats/events. The log stream should be in syslog format and sent to an IP of GSA's choosing.
- Provide GSA full read access to GSA’s data/policies in the firewalls so GSA can audit firewall policies and other data in real time, if desired. (GSA is not requesting access to the contexts of other users).
- Accept firewall policy changes if/when provided a list by GSA in CSV or Excel format (In other words, the contractor shall be responsible for translating any firewall rules from CSV/Excel format to the applicable firewall commands).
- Use Border Gateway Protocol (BGP) routing to failover between MTIPs sites.

The contractor's MTIPS solution shall meet the requirements described in **Section C.2.8.4 Managed Trusted Internet Protocol Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

[1] The NCR MTIPS location is projected to be moved to the RTP data center location in FY19/FY20 before this task order award.

C.2.4.3.1 Connectivity

The contractor's solution shall meet the connectivity requirements as explained in **Section C.2.8.4.1.3 Connectivity** within the MTIPS section in the EIS contract.

The contractor shall take into consideration GSA's unique connectivity requirements as applicable when designing an MTIPS solution for the agency. The MTIPS solution shall provide seamless connectivity for GSA's networking environments and shall support the agency's traffic traversing to the DHS Einstein Enclave for inspection (i.e., Internet, Extranet, and Cloud traffic). The hosted Einstein Enclave is described and depicted in the MTIPS Context Architecture defined in **Section C.2.8.4.1.1.1 MTIPS Context Architecture** of the EIS contract.

C.2.4.3.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.8.4.1.4 Technical Capabilities** within the MTIPS section of the EIS contract.

The routing of all GSA internet traffic is subject to requirements as described in **Section C.1.8.8 National Policy Requirements** of the EIS contract through a DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities (i.e., deliver to and receive from). Once traffic is received at the EINSTEIN Enclave and processed, it is sent back to GSA's MTIPS contractor for delivery to its destination.

The contractor shall support the requirements for routing of Internet, Extranet, and Cloud traffic to a DHS Einstein Enclave for inspection as defined in **Section C.2.8.4.1.4.2 MTIPS Transport Collection and Distribution Capabilities** of the EIS contract.

C.2.4.3.3 Features

The contractor's solution shall include features as described in **C.2.8.4.2 Features** within the MTIPS section of the EIS contract.

C.2.4.3.4 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in MTIPS **Section C.2.8.4.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.4.4 Managed Security Service (MSS)

GSA requires the provision of MSS to safeguard agency internal networks and systems against ever-evolving security threats. The contractor's MSS solution shall meet the requirements described in **Section C.2.8.5 Managed Security Service** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.4.4.1 Managed Firewall Service – Optional to Buy

Demilitarized Zone (DMZ) Firewalls – The contractor shall transition the perimeter DMZ premises-based firewalls, at the MTIPS gateway locations, to a contractor managed network-based firewall service. The contractor shall oversee device monitoring, event correlation and alerting while providing GSA the relevant feeds necessary for its own security information and event management (SIEM) analysis.

C.2.4.4.2 Palo Alto Firewall – Optional to Buy

The contractor shall transition GSA managed Palo Alto Application firewall appliances, which includes model 3050 firewalls, Palo Alto Networks M-100 Panorama Centralized Management Systems (CMS) appliances, and Palo Alto Networks WF-500 WildFire appliance, to a contractor hosted and managed Palo Alto Application firewall solution. The solution shall support the following:

- All traffic shall pass through the TIC.
- Secure Sockets Layer (SSL)/TLS decryption of traffic to up to 1,250 GSA hosted websites with unique certificates.
- SSL/TLS traffic to be decrypted up to 300,000 concurrent sessions.
- Configured in high Active/Standby High-Availability (HA) mode.
- Provide additional subscriptions to:
    - Threat Prevention
    - WildFire
    - URL Filtering
- Develop installation, configuration, and cutover strategies for the Palo Alto Application firewalls and Panorama Centralized Management Systems (CMS).
- Register and License all Palo Alto Networks appliances.
- Perform initial configuration required to enable GUI and CLI management access to all Palo Alto Networks appliances.
- Install the recommended PANOS software and appropriate Palo Alto databases on all Palo Alto Networks appliances.
- Perform management configuration on all Palo Alto Networks appliances.
- Create the appropriate M-100 Templates, Device Groups, Objects, Profiles, and Policy Rules to support the deployment of all appliances
- Assist with the cutover of all the Palo Alto Networks firewalls in Virtual-Wire mode to support inspection and forwarding of live production traffic.
- Monitor network traffic traversing the firewalls to ensure proper handling of the traffic.
- Test appropriate features to ensure proper firewall behavior and troubleshoot any system issues related to the deployment of the firewalls.

As an alternative, the contractor shall host the Palo Alto firewall and GSA would manage the appliance, as a co-location arrangement.

C.2.4.4.3 Connectivity

The contractor's solution shall meet the connectivity requirements as described in **Section C.2.8.5.1.3 Connectivity** within the MSS section in the EIS contract.

C.2.4.4.4 Technical Capabilities

GSA will use MSS to support a wide range of network security requirements to enable GSA and related users to meet mission critical responsibilities.

The agency requires the following MSS capabilities:

- Managed Prevention Service
- Vulnerability Scanning Service
- Incident Response Service

The contractor's service shall include the technical capabilities as described in **Section C.2.8.5.1.4 Technical Capabilities** within the MSS section of the EIS contract and in accordance with Section **C.2.10 Service Related Equipment** of the EIS contract.

C.2.4.4.5 Features

The contractor's solution shall include the features as described in **Section C.2.8.5.2 Features** within the MSS section of the EIS contract.

C.2.4.4.6 Performance Metrics

The contractor's solution shall meet the performance levels as specified in the EIS contract in MSS **Section C.2.8.5.4 Performance Metrics** and **Section G.8.2.1 Service Performance SLAs**.

C.2.4.5 SD-WAN – Optional to Buy

GSA seeks to adopt a hybrid SD-WAN overlay architecture to supplement the EIS contractor managed Layer-3 MPLS network to increase control, security, WAN optimization, and provide additional flexibility for delivery of IT services to all GSA users. The SD-WAN solution will allow GSA with the ability to integrate various WAN access methods (e.g., MPLS/VPNS, Broadband (IPS), Ethernet, (4G/5G) LTE) to provide maximum flexibility for providing greater bandwidth and cost-effective connectivity options at the FOs and redundancy at the ROBs. GSA can deterministically structure how traffic is directed across the available multi-transport connections and to scale network elements based on application flow performance requirements at the FOs and ROBs. It will also simplify the management of the configurations at GSA's remote sites, making it easier and quicker to add broadband and private WAN circuits for increases in bandwidth.

GSA has invested in Cisco/Viptela SD-WAN hardware and expects to have approximately 100 sites deployed at the time of award. GSA has procured a total of 650+ Cisco/Viptela SD-WAN devices to be deployed at all its locations.

The contractor shall have the option to either take ownership of the Cisco/Viptela SD-WAN devices and manage them as MNS or provide equivalent contractor owned and managed universal CPE (uCPE) devices to replace all the Cisco/Viptela devices. If the contractor proposes an SD-WAN solution using replacement uCPE devices, the contractor shall meet all general requirements specified in **Section C.2.4.5.1 General Requirements**. Otherwise, the contractor shall meet all the requirements specified for the SD-WAN solution using the Cisco/Viptela devices in Section **C.2.4.5.2 Cisco/Viptela Requirements**.

C.2.4.5.1 General Requirements

The contractor shall design, install and manage the hybrid SD-WAN overlay solution that shall:

- Be centrally managed via a policy/controller node or other centralized mechanism.
- Allow for the deployment of policy changes via the policy/controller nodes. The policy/controller node shall be accessible by government security personnel to make changes.
- Provide at least two policy/controller nodes for redundancy.
- Provide fully managed SRE and an MNS solution that includes, MPLS/VPNS, broadband (IPS), and wireless (4G/5G LTE) capabilities.
- Provide dynamic traffic engineering that is capable of shifting traffic between circuits based upon latency, hard and soft Quality of Service (QOS) requirements, packet loss and other defined metrics.
- Provide TCP acceleration.
- Provide tiered and burstable connectivity.
- Provide central management to allow deployment of configuration, policy and other changes.
- Utilize uCPE devices to provide virtual switches/routers, WAN optimization, and firewalls.
- Provide orchestration APIs to allow the network to become programmable for service management and enablement and performance and security monitoring, preferably based on open sources..
- Provide multiple connection types such as VPNS/MPLS, dynamic path selection across WAN connections (e.g., to support load sharing).
- Enable multiple VPNs as well as 3rd party services such as WAN optimization controllers, firewalls, and web gateways.
- Provide a simple interface for managing the WAN, using SD-WAN monitoring and management applications.
- Support traffic segregation of GSA's building management system (known as BSN), separated from end-user traffic used for internet access, office automation and productivity applications, VoIP and video/multimedia services.
- Have the ability to scale beyond the existing 800+ field office sites.
- Enable the use of SCADA, Audio Visual (AV) systems, Network Surveillance and Security Systems and Networked Device Management, i.e., IoT.
- Utilize broadband services that terminate into the EIS contractor's MPLS-based VPNS network.
- Utilize OpenFlow (OF) or other interoperable industry standard to enable the controller to directly interact with the forwarding plane of network devices such as switches and routers, both physical and virtual.
- Provide a portal or capability to perform performance analytics.
- Provide 128 and 256 bit encryption.

- Undergo high level Assessment and Authorization (A&A) process for the SD-WAN controllers.

C.2.4.5.2 Cisco/Viptela Requirements

C.2.4.5.2.1 Architect and Engineer an Enterprise-wide SD-WAN Solution

The contractor shall:

- Provide a fully managed SRE and MNS solution using GFE that includes broadband, MPLS and wireless capabilities (4G/5G).
- Architect and design a scalable solution that is centrally managed via Viptela VManage, and VSmart applications. The back-end solution shall consider GSA's pre-existing hosting environments (e.g., Virtual machines hosted at GSA primary colocation data centers or within GSA's Business Services Platform (BSP) hosted within Amazon AWS East/West environment; both are supported with existing FISMA Authority To Operate (ATO) and/or FedRAMP-approved cloud environment. GSA anticipates significant delay if the solution leverages a non-FedRAMP-approved Viptela Cloud.
- Architect a centralized management approach that enables automatic policy/configuration changes, and management and monitoring of the Viptela overlay network (vEdge 100 and vEdge 2000).
- Architect Cisco/Viptela segmentation capability that enables separation of building traffic via centralized policies, which includes the following:
  - Architect Internet protocol security (IPSEC) tunnels via policy using Cisco/Viptela's technology.
  - Architect Cisco/Viptela zero-touch provisioning to allow the devices to be provisioned and configured automatically, eliminating most of the manual labor involved with adding them to a network.
  - Architect an SD-WAN solution using single overlay over T1, MPLS, Broadband or 4G/5G LTE, supporting OSPF, BGP, Virtual Router Redundancy Protocol (VRRP) and Internet Group Management Protocol (IGMP) routing.
  - Architect Cisco/Viptela BGP route redistribution to do the routing.
  - Architect appropriate routing with the Cisco/Viptela Hub controller. Policy rule additions for Cisco/Viptela vEdge devices shall be completed via the Hub controller and pushed to vEdge nodes.
  - Architect Monitoring and Management of Cisco/Viptela's integrated and third-party management capabilities using SNMP and RESTful interfaces.
  - Architect Network Access Control as defined by the government - set appropriate privileges for users or devices accessing the network, including access control limits, as well as appropriate quality of service. Generally follows the user/device as they connect from different parts of the network.
  - Architect Dynamic Interconnects – Creation of dynamic links between locations, including between Data Centers (DCs), enterprise and DCs, and other enterprise locations, as well as dynamically applying appropriate QoS and BW allocation to those links.

  - Architect dynamic Path Control selection for key applications to use policies based on delay sensitivity of the application. Automate configuration of routes via policy.
  - Architect Application Centric Control that identifies applications and enables prioritization of apps based on QoS.
  - Architect automation capabilities inherent to SD-WAN.
  - Architect/engineer monitoring best practices using Cisco/Viptela vManage.
  - Architect global policies via the Cisco/Viptela controller and push those policies to vEdge devices.
- Architect a Cisco/Viptela SD-WAN solution for hub locations in high availability (HA) / redundant mode.
- Architect a Cisco/Viptela SD-WAN solution that scales to support 800+ FO sites.
- Architect, design and engineer a solution with authentication, encryption, and public key infrastructure (PKI). Use Cisco/Viptela's crypto features, including its mechanisms for rekeying and PKI.
- Architect Cisco/Viptela hardware devices for tamper-proofing. Configure location awareness to mitigate social engineering and prevent stealing a box that is shipped to a site from back door access to the GSA corporate network.
- Architect Cisco/Viptela's deep packet inspection (DPI) policies to the fullest extent possible.
- Architect secure SSL/TLS and/or IPSec connections to all components in the network, and to exchange routing, security and policy information.
- Architect policy constructs to manipulate routing information, access control, segmentation, extranets and service chaining.
- Complete tasks in conjunction with government and contractor staff.

C.2.4.5.3 Install and Configure SD-WAN Hub Sites

The contractor shall deploy an architecture for the hub sites to support the overall SD-WAN solution.

The contractor shall:

- Install, configure, test and deploy redundant SD-WAN technology at hub sites and ROBs to facilitate traffic interchange and redundancy.
- The acceptance criteria will be based on a successful testing and validation results for each hub site.
- The acceptance criteria process shall be automated using Cisco/Viptela tools (vManage).
- Design optimal data path for traffic to/from any given site.
- Configure policies for different use cases.
  - **Use Case 1 (Field Site) –** Single or dual pathway BSN and User sites **–** The site policy shall segment traffic from all other GSA traffic. BSN traffic shall be logically isolated from the GSA enterprise network. All BSN building traffic shall be directed to hub firewalls. All traffic shall be encrypted between the edge and hub sites. User traffic shall be separate from building traffic.
  - **Use Case 2 (Field Site) (User only site) –** The site policy shall be configured with encryption between the edge and hub.

  - **Use Case 3 (Field Site) (Dual transport with BSN) –** The site policy shall be configured with encryption between the edge and hub. Applications shall be pinned to either transport that is best appropriate. See use case 1 for requirements.
  - **Use Case 4 (Field Site) (MPLS BSN) –** GSA field sites on managed MPLS that are running BSN. The site policy shall segment traffic from all other GSA traffic. Traffic shall be logically isolated from the GSA enterprise network. All building traffic shall be directed to hub firewalls. Traffic shall be encrypted between the edge and hub sites. User traffic shall be separate from building traffic.
  - **Use Case 5 (Regional Office Building) –** GSA ROBs on managed MPLS running BSN. These locations shall use SD-WAN with broadband as a backup.
- Provide support for existing policies, ports and protocols, such as multicast configurations, QoS.
- Implement the one-time setup for installing the centralized controller and orchestrator.
- Install redundant SD-WAN router at each of the “hub” locations (i.e., data centers and regional offices).
- Develop standard operating procedures (SOPs) for government and contractor to use to maintain and operate system after initial installation.
- Develop a Solution Run Book for each site deployed. The Solution Run Book will contain step-by-step screenshots of the installation and configuration of each hub site.
- Develop a Test Plan for the hubs and the site deployments. The Test Plan shall be re-usable for remaining sites.
- Develop Validation Checklists for the 7 hubs and 100 site deployments.
- Complete tasks in conjunction with government and contractor staff.

C.2.4.5.4 Install Cisco/Viptela SD-WAN at Field Sites and ROBs

The contractor shall install, configure, test and deploy SD-WAN technology at 800+ locations (i.e., ROB, FO). Additionally, the contractor shall:

- Support traffic segregation of GSA’s building management system, known as BSN, separated from end-user traffic used for internet access, office automation and productivity applications, VoIP and video/multimedia services.
- Develop SOPs.
- The acceptance criteria will be based on successful testing and validation results for each site.
- Reduced/on-call near zero-touch support for installing Cisco/Viptela at field sites.

GSA prefers to deploy SD-WAN at Node Type Sites 1-3 as budget and time limitations allow.

C.2.4.5.5 Network Virtualization and Service Chaining (Universal CPE)

GSA anticipates using a uCPE at ROB locations to terminate MPLS and broadband circuits. The initial deployment will be to provide SD-WAN capabilities using MPLS as a primary and broadband as secondary. In the future, GSA may expand the use of the uCPE by taking advantage of service chaining for WAN acceleration and other functions (i.e., IDS, IPS, Firewall capabilities).

The contractor shall:

- Provide Cisco/Viptela SD-WAN software on redundant white box appliances at the ROBs.
- The uCPE shall be capable of supporting WAN acceleration and other software components such firewalls, IDS and IPS.
- The uCPE at the ROBs shall be configured for redundancy and high availability.

C.2.5 Access Arrangements (AA)

Access Arrangements (AA) shall provide the originating and/or terminating access services necessary to connect the SDP to the contractor's POP required to deliver an IT service.

The contractor shall provide AA at the site locations given in **Section J.1-J.2 Pricing Workbooks** of this solicitation. Where no access arrangement is specified, the contractor shall propose appropriate access technologies.

The contractor's AA solution shall meet the requirements described in **Section C.2.9 Access Arrangements** of the EIS contract, as well as any agency-specific requirements detailed in this solicitation.

C.2.5.1 Connectivity

The contractor's solution shall meet the connectivity requirements per **Section C.2.9.1.3 Connectivity** within the AAs section in the EIS contract.

AAs shall connect to and interoperate with:

- Agency-specified locations and equipment
- Contractors network POPs

C.2.5.2 Technical Capabilities

The contractor's solution shall include the technical capabilities as described in **Section C.2.9.1.4 Technical Capabilities** within the AAs section of the EIS contract and in accordance with Section **C.2.10 Service Related Equipment** of the EIS contract. Unless specified in **Section J.1-J.2 Pricing Workbooks** of this solicitation, the contractor shall determine appropriate AA technology and capacity for each agency site.

C.2.5.3 Access Diversity and Avoidance

The contractor shall provide access path diversity and access path avoidance as specified in **Section C.2.9.2** of the EIS contract.

The contractor shall provide diversity options that include, but are not limited to:

- Physically disparate, diverse paths from the SDP to the contractor's POP.
- Redundant paths from an SDP to the contractor's POP.

When necessary to fulfill an order, the contractor shall perform site surveys of potential operational locations to collect and validate floor plans, physical measurements, building power capacity, and external ingress/egress factors. The contractor shall deliver site survey reports after the completion of the physical site visits. Refer to **Section J.10** of the EIS contract for the special access construction template for the site survey report.

Special construction may involve providing a special service or facility related to the delivery and/or performance of a service requirement. This shall include the following situations:

- An access arrangement does not exist or does not have sufficient capacity, and the contractor must provide special construction through the implementation, rearrangement or relocation of physical plant solely for the government-requested access arrangement.
- The contractor uses special construction to implement a different route (government premises to a PCL, PCL to an alternate contractor's POP, or some other type of route) than that which the contractor would otherwise use to provide an access arrangement for the government.

If and when required, special construction will be executed via a TO modification.

C.2.6 Service Related Equipment – Optional to Buy

The contractor shall provide various networking related equipment as specified in **Section C.2.10** of the EIS contract such as switches, routers, telephones, servers, security appliances, firewalls, and wireless devices. The contractor shall provide hardware and materials that are incidental to the installation, operations and maintenance of the EIS services.

The contractor shall leverage and manage the WAN GFE (see **Section C.2.4.1** of this solicitation), as described in **Section G.7** of this solicitation, until a refresh is required. The contractor shall work collaboratively with GSA to define a process to identify which end-of-life equipment needs to be replaced and the timeline to implement the replacements.

The contractor shall install SRE as required to meet the specifications of the terminal equipment located at the government SDP. The details and specifications for the interfaces at each SDP will be provided in the service order.

The SRE required to deliver the services under this solicitation may be purchased by monthly installment for a fixed period of either 36 or 48 months. The SRE to be provided by the contractor shall be new and not refurbished.

The contractor shall meet and comply with the requirements for payment methods as described in **Section B.2.10.4 Payment Methods** of the EIS contract.

C.2.7 Service Related Labor – Optional to Buy

When required, the contractor shall provide qualified staff proficient in network management, LAN/WAN engineering, data and communications, or voice communication systems as appropriate to implement and support the services specified in this solicitation.

C.2.8 Cable and Wiring Service

The contractor shall provide required connectivity using appropriate cabling and wiring, and related trenching, ducting, grounding, and lightning protection systems in accordance with **Section C.12** of the EIS contract and appropriate standards.

C.2.9 National Security and Emergency Preparedness (NS/EP)

The contractor shall adhere to the National Security and Emergency Preparedness requirements as specified in the **Section G.11** of the EIS Contract, National Security and Emergency Preparedness.

C.2.10 Miscellaneous Task Order Unique Requirements

The contractor shall provide the following Task Order Unique CLINs:

- Expedite TUC. Expedite order without local coordination: 10 business days.
- Expedite TUC. Expedite order with local coordination for the following services: IPS, PLS, VPNS: 23 business days for DS3 and below; 30 days above DS3.
- Move TUC. Move a service within a building.
- Move TUC. Move a service within the same CBSA.

C.3.0 Security Requirements

The contractor shall meet all requirements included in **Section C.1.8.7 System Security Requirements** of the EIS contract. The contractor shall, in addition, comply with **Section J.4 Security Assessment and Authorization (A&A) (formerly known as Certification and Accreditation [C&A]) Requirements** of this solicitation. The services in **Table C-5** below would normally be included as part of the system security A&A but not assessed individually.

Table C-5 Services that may require an A&A

EIS Service Area	Service	Notes
Data Service	VPNS	These services would normally

	ETS OWS PLS SONETS DFS IPS	be included as part of the system security A&A but not assessed individually
Voice Service	IPVS CSVS TFS CSDS	IPVS require an A&A. The remainder of the Voice Services would normally be included as part of the system security A&A but not assessed individually
Managed Services	MNS UCS MTIPS MSS	These services require an A&A. Note: MNS and MSS could be included within the same A&A provided that all relevant parts of each were included within that A&A. Note regarding MTIPS: This would be part of a system security assessment responsible for the security between the edge of the (GSA) network and the edge of MTIPs. The MTIPs solution itself also has its own security assessment
Access Arrangements	Access Arrangements	These services would normally be included as part of the system security A&A but not assessed individually
Service Related Equipment	Service Related Equipment	Equipment would normally be included as part of the system security A&A but not assessed individually
Cable and Wiring	Cable and Wiring	Cable and Wiring would normally be included as part of the system security A&A but not assessed individually

The contractor shall also comply with the personnel security requirements below.

C.3.1 Personnel Background Investigation Requirements

The contractor will require access to government buildings, sensitive information and/or access to government information systems. All contractor personnel must successfully complete, at a minimum, a public trust background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1 and GSA Directive 9732.1 Suitability and Personnel Security for background investigations to provide services under this contract. The required background investigations for simple administrative (low risk) personnel shall be a minimum of a Tier 1(T1, formerly - National Agency Check with Written Inquiries (NACI) and for technical staff, personnel who handle Personal Identifiable Information (PII), government sensitive information (not available to the public) or acquisition sensitive information shall complete a Tier 2 (T2S, formerly Moderate Risk Background Investigation - MBI) background investigation or higher depending upon their access and control over the information / systems. The GSA Contracting Officer Representative (COR) shall identify all individuals who require building access, system accounts and verify that they have successfully completed the required background investigations prior to providing them access to government buildings, sensitive information or information systems. To begin work on a contract / task order a contractor must receive **at least an Enter on Duty Determination (EoDD**) or a Final Fit Determination (final adjudication) notification. Background investigation documentation, guidance, and procedures will be provided by the COR and appropriate personnel security analysts.

The contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a federal information system.

C.3.2 Protection of Government Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of this contract. The contractor shall implement procedures that ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive government information, data, and/or equipment. The contractor's procedures shall be consistent with government and GSA policies, including GSA Order 2100.1, Information Technology Security Policy, OMB Circular A-130, Management of Federal Information Resources, OMB M-06-16, OMB M-07-16, HSPD-12, and the Privacy Act. In addition, during all activities and operations on government premises the contractor shall comply with the procedures, policies, rules, and regulations governing the conduct of personnel or protection of government facilities and data as expressed by GSA, written or oral.

All contractor personnel shall take the annual GSA IT Security Awareness Training Course before being allowed access to FAS computers and networks.

The contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a federal information system.

C.4 Transition and Implementation Plan

The contractor shall transition and transform services onto the EIS contract in an efficient and orderly manner. The contractor shall explain in their response how they can accomplish a transition and transformation of GSA services to the EIS contract before the expiration of GSA Networx, WITS, and LSA contracts, with minimal disruption and as economically as possible.

The requirements for transition support are in addition to the EIS Transition requirements as described in **Section C.3.1.2: Contractor's Role in Transition** of the EIS contract.

Transition support shall include two components:

- "**Transition-On**" as defined in **Section C.3** of the EIS contract, including all services provided under GSA's Networx, WITS 3 and LSA contracts.
- "**Transition-Off**" as defined in **Section C.3** of the EIS contract, and will include all services procured under these task order(s).

C.4.1 Transition Approach

The contractor shall describe their transition approach in their proposal. This differs from the Transition-On Plan, described in the following **Section C.4.2**, which will be required from the awarded contractor.

The transition approach shall describe the overall approach to transition and how the contractor can meet a transition deadline of May 31, 2021 for like for like services in task orders 1 and 2, March 31, 2022 for transformation in task orders 1 and 2 and a transition deadline of July 30, 2020 for task order 3.. Some of the items to be discussed in the transition approach are:
How the contractor intends to manage transition risk

- If the contractor has a method of re-using existing circuit facilities and inside wiring.
- Service cutover processes.
- Process for transitioning services from other carriers including the use of back office transition methodologies.

C.4.2 Transition Plan

Within 30 calendar days after the award of the task order(s), the contractor shall provide a detailed transition plan, as described below in **Section C.4.2.1**, for transitioning services to the EIS contract.

The transition plan shall identify significant activities, milestones, risks, and associated mitigations for the "Transition-On" effort. It shall include a matrix listing the major responsibilities for GSA and the contractor to execute during the transition. The transition plan shall have a start date beginning on award date of the TO(s) and shall have a completion date no later than May 31, 2021 for like for like services in task orders 1 and 2, March 31, 2022 for transformation in task orders 1 and 2 and a transition deadline of July 30, 2020 for task order 3.

The transition plan shall be finalized after GSA accepts the proposed plan.

C.4.2.1 Transition-On Plan

- The contractor shall provide and manage a detailed Transition-On Plan and a Transition Quality Plan (TQP) to ensure that the new TO is in place in a thorough and orderly manner within 30 calendar days or less.
- The contractor shall assign an experienced transition project manager(s) to manage all aspects of the Transition-On Plan and TQP to transfer knowledge, tools, documentation, equipment, processes and methodology from the current contractors to the new contractor and their team.
- The contractor's Transition-On Plan shall include:
  - A description of the project management methodology being proposed (e.g., agile, waterfall) and how the selection and implementation is designed to ensure success.
  - A detailed work break-down structure with intermediate and major milestones.
  - A list of all major milestones and deliverables.
  - A list of costs associated with each major milestone.
  - Processes and standards used to ensure meeting agency objectives during the transition.
  - A list of all required items from GSA.
  - Testing contractor operational processes for verification of full operational capability.
  - Governance methods, to include regular reporting to GSA.
- The TQP shall include:
  - A quality-control program.
  - Quality-monitoring tools and techniques.
  - A performance management system and processes.
  - Customer-feedback collection and monitoring methods, tools and techniques.
  - Quality-reporting plans and processes.
  - Corrective-action process, if necessary.

The Transition-On Plan and TQP requirements are only applicable to TOs 1 and 2.

C.4.2.2 Transition-Off Plan

The contractor shall develop and provide a sample detailed Transition-Off Plan based on project management methodologies to be reviewed and accepted by GSA 120 days prior to the start of the last option year. Upon review and acceptance of the Transition-Off Plan, the contractor shall execute the plan.

The Transition-Off Plan requirement is only applicable to TOs 1 and 2.

C.4.3 Transition Management Report

The contractor shall provide a monthly Transition Management Report for status reporting of "Transition On" activities as described below. The report shall include, at a minimum, item counts for:

- Total "Transition On" inventory by service
- EIS orders placed by service
- EIS orders that are delayed or experiencing issues with a short explanation of the issue.

This report shall be delivered to the COR 10 days after the close of each month.

The Transition Management Report requirement is only applicable to TOs 1 and 2.

C.4.4 Implementation Support

The contractor shall perform activities necessary to implement services for GSA as defined in **Section C.3.2** of the EIS contract.

C.4.5 Planning and Coordination

The contractor shall perform planning and coordination activities with GSA and its designated contractors, as required, to implement services for GSA.

C.4.6 Site Surveys and Engineering

The contractor shall be responsible for all site surveys (in-person or virtual) and all engineering for all services installed when requested in the service orders.

C.4.7 Inside Wiring and Demarc Extensions

The contractor shall be responsible for all inside wiring and demarc extensions for all services installed when requested in the service orders. In rare cases, where specific building access issues arise, the contractor shall provide the specific technical requirements to complete the primary service order.

C.4.8 Implementation Testing

The contractor shall comply with Implementation and Testing as described in **Section G.3.4** of the EIS contract.

C.4.9 Implementation Documentation

The contractor shall provide "as-built" engineering drawings and diagrams anytime modifications are made to GSA facilities, such as the installation or removal of wiring or any communications related equipment. Detailed, industry standard drawings, in commonly acceptable format, such as .dwg and .pdf shall be provided, and approved before construction. Formats and methodology shall be coordinated between GSA and the contractor.

C.5 Order Workflow Management

C.5.1 Service Order Submission

GSA requires the capability to place service orders directly with the contractor through GSA's Conexus system and/or the contractor's portal. The contractor shall accept service orders from the GSA Conexus application by web service using the format and specifications provided by GSA Conexus. The contractor shall also accept an order for service in file formats to be provided by GSA. The file could be a spreadsheet or other flat file format delivered via email as an attachment, a secure file transfer, or a manual order entry screen(s). Method of submission is at the sole discretion of GSA. The contractor shall provide a Service Order Acknowledgement (SOA) in accordance with the EIS contract.

All service order placements shall be placed in accordance with **Section G.3.3** of the EIS contract.

C.5.2 Service Order Approval Process

Contractors shall refer to the requirements in **Section G.3.3** of the EIS contract.

C.5.3 Service Order Status

The contractor shall refer to the requirements in Section G.3 and G.5.3.1 of the EIS contract.

C.5.4 Service Order Completion Acceptance

- The contractor shall implement a comprehensive process to ensure services are correctly installed, implemented and tested with GSA prior to service acceptance and that GSA approvals are obtained throughout the process.
- The contractor's service order completion and billing processes shall be in accordance with Sections G and J of the EIS contract.

C.5.5 Service Order Moves, Adds, Changes and Disconnects

- The contractor shall provide a method to bulk upload service order requests by being able to select inventory items to auto-populate service order requests.
- The contractor shall ensure moves, adds, and changes follow the same flow as outlined for service creation.
- The contractor shall ensure the disconnection order due date is auto-populated with the contract's minimum disconnect order interval, and ensure GSA is able to edit this auto-populated field.

The Service Disconnection Order Approval shall use the date GSA designated authority approves the disconnection, and billing shall end on the requested service disconnect date unless GSA approves otherwise.

C.6 Program Management

The contractor shall implement, and follow industry-standards and proven processes to provide Program Management Services in compliance with **Section G.9** of the EIS contract. The contractor shall provide GSA with dedicated support to plan, coordinate, and oversee the transition to the EIS contract and ongoing support for service orders, changes, deletions, and upgrades. The contractor shall provide program management functions including but not limited to: program control, planning at the task order level, contractor performance, resource management, service assurance, reporting and reviews, and senior-level communications.

C.6.1 Task Order Project Plan

The contractor shall provide a Task Order Project Plan (TOPP) based on the site transition sequence to be provided by GSA. The TOPP shall comply with Section **G.3.3.3.3** of the EIS contract. The contractor shall update the TOPP as required by GSA, and on an annual basis.

The TOPP requirement is only applicable to TOs 1 and 2.

C.6.2 Quality Management Plan

The contractor shall develop, maintain, and implement a Quality Management Plan (QMP) describing how the contractor shall ensure that all services delivered meet performance standards and that deliverables meet requirements for timeliness, accuracy, and completeness. The Quality Management Plan shall address the management approach to formulating and enforcing work and quality standards, taking corrective actions as necessary, measuring performance and ensuring compliance with SLAs, providing customer support, performing continuous improvement, and reviewing work-in-progress and deliverables. The contractor shall update the QMP as required by GSA, and on an annual basis.

C.6.3 Communications Plan

The contractor shall provide and implement a detailed Communication Plan describing its management of the day-to-day operations and performance of GSA's network and services. The Communication Plan shall delineate the processes involved in communicating with stakeholders and the incumbent contractors, escalating technical issues, providing customer education, reporting status, conducting meetings, and submitting and maintaining deliverables and other documentation related to GSA's network project. The contractor shall update the Communications Plan as required by GSA, and on an annual basis.

The Communications Plan requirement is only applicable to TOs 1 and 2.

C.6.4 Kick-Off Meeting

Within 10 business days of TO award(s), the contractor shall conduct a project kick-off meeting with GSA, at the 1800 F St, NW, Washington, DC facility. The contractor shall develop and share an agenda with GSA two business days prior to meeting. The kick-off meeting shall include the following agenda items:

- Establishing a collaborative team environment and clear communication paths
- Discussion of contract and technical transition-in activities, including issues, risks and mitigations
- Establishing a clear understanding of GSA's near-term and longer-term system and technical objectives, challenges, relevant stakeholders, and specific expectations for contractor engineering and operational support
- Establishing clear understanding of GSA expectations for strategic and leadership support from the contractor's Program Manager and any other key personnel

The contractor Program Manager and all contractor key personnel shall attend the kick-off meeting in person. The contractor shall provide meeting notes from the kick-off meeting, and track the progress and completion of all assigned action items.

C.6.5 Project Review Meetings

The contractor, and any necessary subcontractors, shall plan and facilitate Project Review Meetings when requested by GSA. The contractor shall develop and share an agenda with GSA two business days prior to meeting. The contractors shall participate in these Project Review Meetings either in person or via teleconference, at the direction of the Ordering Contracting Officer (OCO). The topics covered at each Project Review Meeting will include, but are not limited to, the following:

- Review of the most recent Transition Management Report
- Overall project schedule and milestones
- Current risk assessment and mitigation strategies
- Issues and resolution
- Previous action items and status
- Deliverables submitted during the preceding week and upcoming deliverables, and
- Status of task order modifications

The contractor shall provide meeting notes for all meetings, and track the progress and completion of all assigned action items.

The Project Review Meeting requirement is only applicable to TOs 1 and 2.

C.6.6 Miscellaneous Meetings

The contractor, and any necessary subcontractors, shall participate in other miscellaneous meetings as requested by GSA. The contractor shall develop and share an agenda with GSA two business days prior to meeting. The contractor, and any necessary subcontractors, shall plan and initiate other meetings proactively, as needed. The contractor shall provide meeting notes for all meetings, and track the progress and completion of all assigned action items.

The miscellaneous meetings requirement is only applicable to TOs 1 and 2.

C.6.7 Risk Management

The network provided by the contractor supports successful operation of GSA's network infrastructure and services provided to its 14,000 end-users and a number of external agencies. Given the importance of ensuring highly available and operable services for all of GSA users, it is vital that the contractor place high emphasis on managing and mitigating operational risks to the contractor's network and services.

A risk is a possible future event that may impact the cost, schedule, or operational quality of the service delivered by the contractor. Proactive assessment and mitigation of risks is crucial for successful execution of network services. The contractor shall develop and implement a Risk Management Plan (RMP) at the overall task order level, as well as for specific network component transition, implementation and operation.

The contractor shall update the RMP as required by GSA, and on an annual basis.

The RMP requirement is only applicable to TOs 1 and 2.

C.7 Section 508 Accessibility

The contractor shall adhere to the Section 508 requirements as specified in **Section C.4** of the EIS Contract.